UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/762,330	01/23/2004	Satoru Tanaka	1046.1306	4953

21171 7590 10/25/2010

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
10/25/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/762,330	TANAKA, SATORU	
	Examiner	Art Unit	
	BENJAMIN E. LANIER	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 March 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 16 March 2010 has been entered.

Response to Amendment

2. Applicant's amendment filed 16 March 2010 amends claims 1, 3-5, 7-9, 11-13, 15, 17, 18, 20, 22, 24, 26, and 27. Claims 29 and 30 are added. Applicant's amendment has been fully considered and entered.

Response to Arguments

3. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the client computer system can still access non-protected data through the gateway server when the anti-virus data file is not updated) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

4. Applicant argues, "Hermann fails to disclose, either expressly, or inherently by failing to necessarily require, the language of amended claim 1, namely '***to restrict as a restriction range an access permission range on a network [[by]] of the user apparatus to be within a range on a network to which a security setting guide server management device belongs***." This argument

is not persuasive because Herrmann discloses that if the client computer is determined to be non-compliant, a sandbox server can provide access to the required anti-virus updates or information about where such updates may be obtained ([0051]). This recitation is sufficient to meet the claimed limitations because Applicant's specification discloses that the claimed access permission range provides for the updated virus definition files (Page 10, lines 10-24).

5. Applicant argues, "nothing has been cited or found in Herrmann that expressly or inherently (necessarily) discloses the limitations of independent claim 15. For example, Herrmann is silent on '***port access information of the user terminal***' and/or '***responsive to a command by the user terminal***' for determining a security level of the user terminal." In response, claim 15 requires that the security level of a user terminal is determined based upon one or more of a plurality of claim elements. Therefore, only one claim element from the list needs to be addressed.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-30 are rejected under 35 U.S.C. 102(e) as being anticipated by Herrmann, U.S. Publication No. 2003/0055994. Referring to claims 1, 5, 9, 13, 19, 21, 23, 28, Herrmann discloses providing anti-virus cooperative enforcement wherein network access is permitted/denied based upon whether the client computer virus definition files are updated

([0050] & [0071] & [0073] & [0076] & [0081]), which meets the limitation of a security management device, an apparatus for a user and a security setting guide device in communication via a network, security detection unit detecting a security level of a user application based upon an access record of the user apparatus accessing a virus information computer, a judging unit judging whether the security level of the user apparatus reaches a predetermined security level, the detecting is based upon whether the user apparatus accesses the virus information computer at a predetermined level. Herrmann discloses that if the client computer is determined to be non-compliant, a sandbox server can provide access to the required anti-virus updates or information about where such updates may be obtained ([0051]), which meets the limitation of an access control unit, in case the judging unit judges the security level of the user apparatus does not reach the predetermined security level, to restrict as a restriction range an access permission range on a network of the user apparatus to be within a range on network to which a security setting guide server management device belongs.

Referring to claims 2, 6, 10, 20, 22, 24, Herrmann discloses that if the client computer is determined to be complaint, the client is permitted access to the network ([0050]), which meets the limitation of the access control unit, in case the judging unit judges that the security level of the user apparatus reaches the predetermined level, sets a range wider than the restriction range as the access permission range of the user apparatus, in case the judging unit judges that the security level of the user apparatus has reached the predetermined security level, does not restrict the access permission range on the network by the user apparatus.

Referring to claims 3-4, 7-8, 11-12, 14, Herrmann discloses that if the client computer is determined to be non-compliant, a sandbox server can provide access to the required anti-virus

updates or information about where such updates may be obtained ([0051]), which meets the limitation of the access control unit has a function of controlling a communication route of the user apparatus and, in case the judging unit judges that the security level of the user apparatus does not reach the predetermined level, as the restriction range controls a communication destination of the user apparatus to the security setting guide server management device, the security setting guide server management device controls updating the virus definition file of the user apparatus, in case the judging unit judges the security level of the user apparatus does not reach the predetermined security level, connects the user apparatus to the security setting guide device.

Referring to claims 15, 18, 25, 27, Herrmann discloses providing anti-virus cooperative enforcement wherein network access is permitted/denied based upon whether the client computer virus definition files are updated ([0050] & [0071] & [0073] & [0076] & [0081]), which meets the limitation of determining a security level of a user terminal upon a network access for the user terminal, based upon an access record of the user terminal access a virus information computer, security information updating history of the user terminal, and ensuring a predetermined security level on the network, according to the determined security level of the user terminal, the security information comprises a virus definition file and the security information updating history of the user terminal comprises an access pattern to a security information server for updating security information and/or an access history to the security information for updating the security information, the user apparatus is established to afford the network. Herrmann discloses that if the client computer is determined to be non-compliant, a sandbox server can provide access to the required anti-virus updates or information about where

such updates may be obtained ([0051]), which meets the limitation of wherein when a security level of the user terminal does not reach the predetermined security level, the ensuring of the predetermined security level includes restricting an access permission range on a network of the user terminal to be within a range on network to which a specified device belongs, the restricting of an access permission range on the network of the user terminal includes controlling a communication destination of the user terminal to a security setting guide server management device.

Referring to claim 17, Herrmann discloses that if the client computer is determined to be non-compliant, a sandbox server can provide access to the required anti-virus updates or information about where such updates may be obtained ([0051]), which meets the limitation of the ensuring of the predetermined security level on the network comprises guiding by the specified device the user terminal to meet the predetermined security level.

Referring to claim 26, Herrmann discloses that if the client computer is determined to be complaint, the client is permitted access to the network ([0050]), which meets the limitation of in case the judging unit judges that the security level of the user apparatus has reached the predetermined security level, the ensuring of the predetermine security level includes not restricting an access permission range on the network of the user apparatus.

Referring to claims 29-30, Herrmann discloses providing anti-virus cooperative enforcement wherein network access is permitted/denied based upon whether the client computer virus definition files are updated ([0050] & [0071] & [0073] & [0076] & [0081]), which meets the limitation of security detection unit to detect a security level of a user apparatus based upon a virus definition file of the user apparatus, a judging unit to judge whether the security level of the

user apparatus reaches a predetermined security level. Herrmann discloses that if the client computer is determined to be non-compliant, a sandbox server can provide access to the required anti-virus updates or information about where such updates may be obtained ([0051]), which meets the limitation of an access control unit to restrict as a restriction range an access permission range on a network of the user apparatus to be within a range on network to which a security setting guide server management device belongs, the access control unit restricts the user apparatus to access and/or become accessible to apparatuses within the first range on the network including the security management device and an apparatus that provides the virus definition file to the user apparatus. Herrmann discloses that if the client computer is determined to be complaint, the client is permitted access to the network ([0050]), which meets the limitation of set the access permission range on the network to a second range that exceeds the first range when the judging unit judges the security level of the user apparatus reaches the predetermined security level.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN E. LANIER whose telephone number is (571)272-3805. The examiner can normally be reached on M-Th 7:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432